One Identity Manager 8.2

# Administrationshandbuch für die Datenarchivierung

**Legende**

**WARNUNG: Das Symbol WARNUNG weist auf ein potenzielles Risiko von Körperverletzungen oder Sachschäden hin, für das Sicherheitsvorkehrungen nach Industriestandard empfohlen werden. Dieses Symbol ist oft verbunden mit elektrischen Gefahren bezüglich Hardware.**

**VORSICHT: Das Symbol VORSICHT weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.**

One Identity Manager Administrationshandbuch für die Datenarchivierung
Aktualisiert - 24. November 2021, 11:09 Uhr
Version - 8.2

# Inhalt

# Archivierung der Datenänderungen

Alle im One Identity Manager erfassten Datenänderungen werden zunächst in der One Identity Manager-Datenbank gespeichert. Historische Daten der One Identity Manager-Datenbank werden in zyklischen Abständen in eine One Identity Manager History Database übertragen. Diese One Identity Manager History Database stellt somit das Veränderungsarchiv dar. In der One Identity Manager History Database erfolgen statistische Auswertungen, die die Darstellungen von Trends oder Verläufen vereinfachen. Die Auswertung der historischen Daten erfolgt über die TimeTrace-Funktion oder über Berichte.

Die Einrichtung einer Arbeitsumgebung für eine One Identity Manager History Database umfasst folgende Schritte:

- Einrichten einer administrativen Arbeitsstation
- Erstellen und Migrieren der One Identity Manager History Database
- Installieren und Konfigurieren eines One Identity Manager Service für die One Identity Manager History Database
- Bekanntgeben der Quelldatenbank
- Einrichten des Archivierungsverfahrens

### Detaillierte Informationen zum Thema

- Inbetriebnahme einer One Identity Manager History Database auf Seite 5
- Quelldatenbanken in der One Identity Manager History Database bekanntgeben auf Seite 28
- Einrichten des Archivierungsverfahrens auf Seite 30

# Inbetriebnahme einer One Identity Manager History Database

Alle im One Identity Manager protokollierten Aufzeichnungen werden zunächst in der One Identity Manager-Datenbank gespeichert. Die Aufzeichnungen sollten in regelmäßigen Abständen aus der One Identity Manager-Datenbank entfernt und in einer One Identity Manager History Database archiviert werden.

Die aufgezeichneten Daten unterliegen unter Umständen weiteren Regularien wie beispielsweise gesetzlichen Aufbewahrungsfristen. Es wird empfohlen One Identity Manager History Databases entsprechend der Berichtszeiträume zu betreiben. Nach Ablauf eines definierten Berichtszeitraums kann eine neue One Identity Manager History Database eingerichtet werden.

Abhängig vom Datenvolumen der One Identity Manager-Datenbank, den zu archivierenden Daten und deren Änderungshäufigkeit kann es erforderlich sein, in gewissen Zeitabständen (beispielsweise jährlich, quartalsweise oder monatlich) weitere One Identity Manager History Databases zu erstellen. Der Anteil der historisierten Daten am Gesamtvolumen einer One Identity Manager-Datenbank sollte maximal 25 % betragen. Anderenfalls kann es zu Performance-Problemen kommen.

### Detaillierte Informationen zum Thema


- Berechtigungen für die One Identity Manager History Database auf einem SQL Server auf Seite 6
- Berechtigungen für die One Identity Manager History Database in einer verwalteten Instanz in Azure SQL-Datenbank auf Seite 11
- Erweiterte Konfiguration für die Datenübernahme auf Seite 15
- Hinweise zum Einsatz mehrerer SQL Server auf Seite 18
- Hinweise zur Nutzung der integrierten Windows-Authentifizierung auf Seite 19
- Einrichten eines One Identity Manager Service für die One Identity Manager History Database auf Seite 20
- Einrichten einer administrativen Arbeitsstation für den Zugriff auf die One Identity Manager History Database auf Seite 21

- Installieren einer One Identity Manager History Database auf Seite 23
- Ablauf der Aktualisierung bei Freigabe einer neuen Version auf Seite 25

# Berechtigungen für die One Identity Manager History Database auf einem SQL Server

Für den Einsatz einer One Identity Manager History Database auf einem SQL Server mit dem abgestufte Berechtigungskonzept werden folgende Benutzer unterschieden. Die Berechtigungen der Benutzer auf Serverebene und Datenbankebene sind auf ihre Aufgaben abgestimmt.

HINWEIS: Wenn Sie bei der Aktualisierung von Version 8.1.x zu abgestuften Berechtigungen wechseln möchten, wenden Sie sich an den Support. Das Support Portal ist unter https://support.oneidentity.com/identity-manager/ erreichbar.

- Installationsbenutzer

  Der Installationsbenutzer wird für die initiale Installation einer One Identity Manager History Databasemit dem Configuration Wizard benötigt.

  HINWEIS: Wenn Sie bei der Aktualisierung von Version 8.0.x auf die Version 8.2 auf das abgestufte Berechtigungskonzept wechseln möchten, benötigen Sie ebenfalls diesen Installationsbenutzer.

- Administrativer Benutzer

  Der administrative Benutzer wird durch Komponenten des One Identity Manager verwendet, die Berechtigungen auf Serverebene und Datenbankebene benötigen, beispielsweise der Configuration Wizard, der DBQueue Prozessor oder der One Identity Manager Service.

- Konfigurationsbenutzer

  Der Konfigurationsbenutzer kann Konfigurationsaufgaben innerhalb des One Identity Manager ausführen, beispielsweise mit dem Designer arbeiten. Konfigurationsbenutzer benötigen Berechtigungen auf Serverebene und Datenbankebene.

- Endbenutzer

  Endbenutzer erhalten nur Berechtigungen auf Datenbankebene, um beispielsweise Aufgaben mit dem HistoryDB Manager zu erfüllen.

Ausführliche Informationen zu den minimalen Berechtigungsebenen der One Identity Manager-Werkzeuge finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

## Berechtigungen für den Installationsbenutzer

Für den Installationsbenutzer müssen eine SQL Server Anmeldung und ein Datenbankbenutzer mit den folgenden Berechtigungen zur Verfügung gestellt werden.

SQL Server:

- Mitglied der Serverrolle **dbcreator**

  Die Serverrolle wird nur benötigt, wenn die Datenbank durch den Configuration Wizard erstellt wird.

- Mitglied der Serverrolle **sysadmin**

  Diese Serverrolle wird nur benötigt, wenn die Datenbank durch den Configuration Wizard erstellt wird und dabei die Verzeichnisse für die Dateien über den Dateibrowser gewählt werden müssen. Werden die Dateien in den Standardverzeichnissen des Datenbankservers abgelegt, wird die Berechtigung nicht benötigt.

- Mitglied der Serverrolle **securityadmin**

  Diese Serverrolle wird für die Erstellung der SQL Server Anmeldungen benötigt.

- Berechtigung **view server state** mit der Option **with grant option** und Berechtigung **alter any connection** mit der Option **with grant option**

  Die Berechtigungen werden zum Prüfen von Verbindungen und gegebenenfalls Schließen von Verbindungen benötigt.

- Berechtigung **alter any server role**

  Die Berechtigung wird benötigt, um die Serverrolle für den administrativen Benutzer zu erzeugen.

msdb-Datenbank:

- Berechtigung **Select** mit der Option **with grant option** für die Tabellen `dbo.sysjobs`, `dbo.sysjobschedules`, `dbo.sysjobactivity`, `dbo.sysschedules` und `dbo.sysjobhistory`

  Die Berechtigungen werden zum Ausführen und Überwachen von Datenbankschedules benötigt.

- Berechtigung **alter any user**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankbenutzer für den administrativen Benutzer benötigt.

- Berechtigung **alter any role**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankrollen für den administrativen Benutzer benötigt.

master-Datenbank:

- Berechtigung **alter any user**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankbenutzer für den administrativen Benutzer benötigt.

- Berechtigung **alter any role**

Die Berechtigung wird zum Erzeugen der benötigten Datenbankrollen für den administrativen Benutzer benötigt.

- Berechtigung **Execute** mit der Option **with grant option** für die Prozedur `xp_readerrorlog`

  Die Berechtigung wird benötigt, um Informationen zum Systemstatus des Datenbankservers zu ermitteln.

- Mitglied der Datenbankrolle **SQLAgentUserRole**

  Die Datenbankrolle wird zum Verwalten von Datenbankschedules während der Aktualisierung von Version 8.0.x auf die Version 8.2 benötigt.

One Identity Manager History Database:

- Mitglied der Datenbankrolle **db_owner**

  Diese Datenbankrolle wird benötigt, wenn bei der Installation des Schemas mit dem Configuration Wizard eine vorhandene Datenbank verwendet werden soll oder eine Aktualisierung des Schemas erfolgt.

## Berechtigungen für den administrativen Benutzer

Für den administrativen Benutzer werden während der Installation einer One Identity Manager History Databasemit dem Configuration Wizard folgende Prinzipale mit den Berechtigungen erstellt:

SQL Server:

- Serverrolle **OneIMAdminRole_<DatabaseName>**
  - Berechtigung **alter any server role**

    Die Berechtigung wird benötigt, um die Serverrolle für den Konfigurationsbenutzer zu erzeugen.
  - Berechtigung **view any definition**

    Die Berechtigung wird benötigt, um die SQL Server Anmeldungen für den Konfigurationsbenutzer und den Endbenutzer mit den entsprechenden Datenbankbenutzern zu verbinden.
- SQL Server Anmeldung **<DatabaseName>_Admin**
  - Mitglied der Serverrolle **OneIMAdminRole_<DatabaseName>**
  - Berechtigung **view server state** mit der Option **with grant option** und Berechtigung **alter any connection** mit der Option **with grant option**

    Die Berechtigungen werden zum Prüfen von Verbindungen und gegebenenfalls Schließen von Verbindungen benötigt.

msdb-Datenbank:

- Datenbankrolle **OneIMRole_<DatabaseName>**
  - Mitglied der Datenbankrolle **SQLAgentUserRole**

    Die Datenbankrolle wird zum Ausführen von Datenbankschedules benötigt.

        - Berechtigung **Select** für die Tabellen `dbo.sysjobs`, `dbo.sysjobschedules`, `dbo.sysjobactivity`, `dbo.sysschedules` und `dbo.sysjobhistory`

          Die Berechtigungen werden zum Ausführen und Überwachen von Datenbankschedules benötigt.
    - Datenbankbenutzer **OneIM_<DatabaseName>**
        - Mitglied der Datenbankrolle **OneIMRole_<DatabaseName>**
        - Der Datenbanknutzer wird der SQL Server Anmeldung **<DatabaseName>_Admin** zugewiesen.

master-Datenbank:

- Datenbankrolle **OneIMRole_<DatabaseName>**
    - Berechtigung **Execute** für die Prozedur `xp_readerrorlog`

      Die Berechtigung wird benötigt, um Informationen zum Systemstatus des Datenbankservers zu ermitteln.
- Datenbankbenutzer **OneIM_<DatabaseName>**
    - Mitglied der Datenbankrolle **OneIMRole_<DatabaseName>**
    - Der Datenbanknutzer wird der SQL Server Anmeldung **<DatabaseName>_Admin** zugewiesen.

One Identity Manager History Database:

- Datenbankbenutzer **Admin**
    - Mitglied in Datenbankrolle **db_owner**

      Die Datenbankrolle wird benötigt, um eine Datenbank mit dem Configuration Wizard zu aktualisieren.
    - Der Datenbanknutzer wird der SQL Server Anmeldung **<DatabaseName>_Admin** zugewiesen.

### Berechtigungen für den Konfigurationsbenutzer

Für Konfigurationsbenutzer werden während der Installation einer One Identity Manager History Databasemit dem Configuration Wizard folgende Prinzipale mit den Berechtigungen erstellt:

SQL Server:

- Serverrolle **OneIMConfigRole_<DatabaseName>**
    - Berechtigung **view server state** und Berechtigung **alter any connection**

      Die Berechtigungen werden zum Prüfen von Verbindungen und gegebenenfalls Schließen von Verbindungen benötigt.
- SQL Anmeldung **<DatabaseName>_Config**
    - Mitglied der Serverrolle **OneIMConfigRole_<DatabaseName>**

One Identity Manager History Database:

- Datenbankrolle **OneIMConfigRoleDB**
  - Berechtigungen **Create procedure**, **Delete**, **Select**, **Create table**, **Update**, **Checkpoint**, **Create view**, **Insert**, **Execute**, **Create function** auf die Datenbank
- Datenbankbenutzer **Config**
  - Mitglied der Datenbankrolle **OneIMConfigRoleDB**
  - Der Datenbankbenutzer wird mit der SQL Server Anmeldung **<DatabaseName>_Config** verbunden.

## Berechtigungen für den Endbenutzer

Für Endbenutzer werden während der Installation einer One Identity Manager History Databasemit dem Configuration Wizard folgende Prinzipale mit den Berechtigungen erstellt:

SQL Server:

- SQL Anmeldung **<DatabaseName>_User**

One Identity Manager History Database:

- Datenbankrolle **OneIMUserRoleDB**
  - Berechtigungen **Insert**, **Update**, **Select**, **Delete** auf ausgewählte Tabellen der Datenbank
  - Berechtigung **view definition** auf die Datenbank
  - Berechtigungen **Execute** und **References** für einzelne Funktionen, Prozeduren und Typen
- Datenbankbenutzer **User**
  - Mitglied der Datenbankrolle **OneIMUserRoleDB**
  - Der Datenbankbenutzer wird mit der SQL Server Anmeldung **<DatabaseName>_User** verbunden.

## Hinweise zur Nutzung der integrierten Windows Authentifizierung

Die integrierte Windows Authentifizierung kann für den One Identity Manager Service und die Webanwendungen uneingeschränkt genutzt werden. Für die Fat-Clients kann die integrierte Windows Authentifizierung genutzt werden. Die Nutzung von Windows Gruppen zur Anmeldung wird unterstützt. Zur Sicherstellung der Funktionalität wird jedoch dringend die Nutzung einer SQL Server Anmeldung empfohlen.

### *Um die integrierte Windows Authentifizierung einzusetzen*

- Richten Sie für das Benutzerkonto auf dem Datenbankserver eine SQL Server Anmeldung ein.

- Tragen Sie als Standardschema **dbo** ein.
- Weisen Sie der SQL Server Anmeldung die benötigten Berechtigungen zu.

# Berechtigungen für die One Identity Manager History Database in einer verwalteten Instanz in Azure SQL-Datenbank

Für den Einsatz einer One Identity Manager History Database in einer verwalteten Instanz in Azure SQL-Datenbank mit dem abgestufte Berechtigungskonzept werden folgende Benutzer unterschieden. Die Berechtigungen der Benutzer auf Serverebene und Datenbankebene sind auf ihre Aufgaben abgestimmt.

- Installationsbenutzer

  Der Installationsbenutzer wird für die initiale Installation einer One Identity Manager History Databasemit dem Configuration Wizard benötigt.

- Administrativer Benutzer

  Der administrative Benutzer wird durch Komponenten des One Identity Manager verwendet, die Berechtigungen auf Serverebene und Datenbankebene benötigen, beispielsweise der Configuration Wizard, der DBQueue Prozessor oder der One Identity Manager Service.

- Konfigurationsbenutzer

  Der Konfigurationsbenutzer kann Konfigurationsaufgaben innerhalb des One Identity Manager ausführen, beispielsweise mit dem Designer arbeiten. Konfigurationsbenutzer benötigen Berechtigungen auf Serverebene und Datenbankebene.

- Endbenutzer

  Endbenutzer erhalten nur Berechtigungen auf Datenbankebene, um beispielsweise Aufgaben mit dem HistoryDB Manager zu erfüllen.

Ausführliche Informationen zu den minimalen Berechtigungsebenen der One Identity Manager-Werkzeuge finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

## Berechtigungen für den Installationsbenutzer

Für den Installationsbenutzer müssen eine SQL Server Anmeldung und ein Datenbankbenutzer mit den folgenden Berechtigungen zur Verfügung gestellt werden.

SQL Server:

- Mitglied der Serverrolle **dbcreator**

  Die Serverrolle wird nur benötigt, wenn die Datenbank durch den Configuration Wizard erstellt wird.

- Mitglied der Serverrolle **securityadmin**

  Diese Serverrolle wird für die Erstellung der SQL Server Anmeldungen benötigt.

- Berechtigung **view server state** mit der Option **with grant option** und Berechtigung **alter any connection** mit der Option **with grant option**

  Die Berechtigungen werden zum Prüfen von Verbindungen und gegebenenfalls Schließen von Verbindungen benötigt.

- Berechtigung **alter any server role**

  Die Berechtigung wird benötigt, um die Serverrolle für den administrativen Benutzer zu erzeugen.

msdb-Datenbank:

- Berechtigung **Select** mit der Option **with grant option** für die Tabellen `dbo.sysjobs`, `sysjobsteps`, `dbo.sysjobschedules`, `dbo.sysjobactivity`, `dbo.sysschedules` und `dbo.sysjobhistory`

  Die Berechtigungen werden zum Ausführen und Überwachen von Datenbankschedules benötigt.

- Berechtigung **alter any user**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankbenutzer für den administrativen Benutzer benötigt.

- Berechtigung **alter any role**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankrollen für den administrativen Benutzer benötigt.

master-Datenbank:

- Berechtigung **alter any user**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankbenutzer für den administrativen Benutzer benötigt.

- Berechtigung **alter any role**

  Die Berechtigung wird zum Erzeugen der benötigten Datenbankrollen für den administrativen Benutzer benötigt.

- Berechtigung **Execute** mit der Option **with grant option** für die Prozedur `xp_readerrorlog`

  Die Berechtigung wird benötigt, um Informationen zum Systemstatus des Datenbankservers zu ermitteln.

- Berechtigung **Execute** mit der Option **with grant option** für die Prozeduren `xp_sqlagent_is_starting`, `xp_sqlagent_notify` und `xp_sqlagent_enum_jobs`

Die Berechtigungen werden zum Ausführen und Überwachen von Datenbankschedules benötigt.

One Identity Manager History Database:

- Mitglied der Datenbankrolle **db_owner**

  Diese Datenbankrolle wird benötigt, wenn bei der Installation des Schemas mit dem Configuration Wizard eine vorhandene Datenbank verwendet werden soll oder eine Aktualisierung des Schemas erfolgt.

## Berechtigungen für den administrativen Benutzer

Für den administrativen Benutzer werden während der Installation einer One Identity Manager History Databasemit dem Configuration Wizard folgende Prinzipale mit den Berechtigungen erstellt:

SQL Server:

- Serverrolle **OneIMAdminRole_<DatabaseName>**
  - Berechtigung **alter any server role**

    Die Berechtigung wird benötigt, um die Serverrolle für den Konfigurationsbenutzer zu erzeugen.
  - Berechtigung **view any definition**

    Die Berechtigung wird benötigt, um die SQL Server Anmeldungen für den Konfigurationsbenutzer und den Endbenutzer mit den entsprechenden Datenbankbenutzern zu verbinden.
- SQL Server Anmeldung **<DatabaseName>_Admin**
  - Mitglied der Serverrolle **OneIMAdminRole_<DatabaseName>**
  - Berechtigung **view server state** mit der Option **with grant option** und Berechtigung **alter any connection** mit der Option **with grant option**

    Die Berechtigungen werden zum Prüfen von Verbindungen und gegebenenfalls Schließen von Verbindungen benötigt.

msdb-Datenbank:

- Datenbankrolle **OneIMRole_<DatabaseName>**
  - Mitglied der Datenbankrolle **SQLAgentUserRole**

    Die Datenbankrolle wird zum Ausführen von Datenbankschedules benötigt.
  - Berechtigung **Select** für die Tabellen `dbo.sysjobs`,`sysjobsteps`, `dbo.sysjobschedules`, `dbo.sysjobactivity`, `dbo.sysschedules` und `dbo.sysjobhistory`

    Die Berechtigungen werden zum Ausführen und Überwachen von Datenbankschedules benötigt.

- Datenbankbenutzer **OneIM_<DatabaseName>**
  - Mitglied der Datenbankrolle **OneIMRole_<DatabaseName>**
  - Der Datenbanknutzer wird der SQL Server Anmeldung **<DatabaseName>_Admin** zugewiesen.

master-Datenbank:

- Datenbankrolle **OneIMRole_<DatabaseName>**
  - Berechtigung **Execute** für die Prozedur `xp_readerrorlog`

    Die Berechtigung wird benötigt, um Informationen zum Systemstatus des Datenbankservers zu ermitteln.
  - Berechtigung **Execute** für die Prozeduren `xp_sqlagent_is_starting`, `xp_sqlagent_notify` und `xp_sqlagent_enum_jobs`

    Die Berechtigungen werden zum Ausführen und Überwachen von Datenbankschedules benötigt.
- Datenbankbenutzer **OneIM_<DatabaseName>**
  - Mitglied der Datenbankrolle **OneIMRole_<DatabaseName>**
  - Der Datenbanknutzer wird der SQL Server Anmeldung **<DatabaseName>_Admin** zugewiesen.

One Identity Manager History Database:

- Datenbankbenutzer **Admin**
  - Mitglied in Datenbankrolle **db_owner**

    Die Datenbankrolle wird benötigt, um eine Datenbank mit dem Configuration Wizard zu aktualisieren.
  - Der Datenbanknutzer wird der SQL Server Anmeldung **<DatabaseName>_Admin** zugewiesen.

## Berechtigungen für den Konfigurationsbenutzer

Für Konfigurationsbenutzer werden während der Installation einer One Identity Manager History Databasemit dem Configuration Wizard folgende Prinzipale mit den Berechtigungen erstellt:

SQL Server:

- Serverrolle **OneIMConfigRole_<DatabaseName>**
  - Berechtigung **view server state** und Berechtigung **alter any connection**

    Die Berechtigungen werden zum Prüfen von Verbindungen und gegebenenfalls Schließen von Verbindungen benötigt.
- SQL Anmeldung **<DatabaseName>_Config**
  - Mitglied der Serverrolle **OneIMConfigRole_<DatabaseName>**

One Identity Manager History Database:

- Datenbankrolle **OneIMConfigRoleDB**
  - Berechtigungen **Create procedure**, **Delete**, **Select**, **Create table**, **Update**, **Checkpoint**, **Create view**, **Insert**, **Execute**, **Create function** auf die Datenbank
- Datenbankbenutzer **Config**
  - Mitglied der Datenbankrolle **OneIMConfigRoleDB**
  - Der Datenbankbenutzer wird mit der SQL Server Anmeldung **<DatabaseName>_Config** verbunden.

### Berechtigungen für den Endbenutzer

Für Endbenutzer werden während der Installation einer One Identity Manager History Databasemit dem Configuration Wizard folgende Prinzipale mit den Berechtigungen erstellt:

SQL Server:

- SQL Anmeldung **<DatabaseName>_User**

One Identity Manager History Database:

- Datenbankrolle **OneIMUserRoleDB**
  - Berechtigungen **Insert**, **Update**, **Select**, **Delete** auf ausgewählte Tabellen der Datenbank
  - Berechtigung **view definition** auf die Datenbank
  - Berechtigungen **Execute** und **References** für einzelne Funktionen, Prozeduren und Typen
- Datenbankbenutzer **User**
  - Mitglied der Datenbankrolle **OneIMUserRoleDB**
  - Der Datenbankbenutzer wird mit der SQL Server Anmeldung **<DatabaseName>_User** verbunden.

# Erweiterte Konfiguration für die Datenübernahme

Für die Datenübernahme von der One Identity Manager-Datenbank in die One Identity Manager History Database gibt es folgende Szenarien, die eine erweiterte Konfiguration erfordern.

## Szenario 1

One Identity Manager History Database und One Identity Manager-Datenbank befinden sich auf einem Datenbankserver.

HINWEIS: Wenn Sie mit dem **sa** arbeiten, sind keine weiteren Schritte erforderlich.

Wenn Sie mit abgestuften Berechtigungen auf Serverebene und Datenbankebene arbeiten, erstellen Sie im Designer in der One Identity Manager-Datenbank einen Datenbankbenutzer für die Datenübernahme.

***Um den Datenbankbenutzer in der One Identity Manager-Datenbank einzurichten***

1. Wählen Sie im Designer die Kategorie **Basisdaten > Sicherheitseinstellungen > Datenbankserverberechtigungen > Datenbankserver-Anmeldungen**.
2. Klicken Sie und erfassen Sie folgende Informationen:
    - **Anmeldename**: SQL Server Anmeldung des Benutzers, mit dem die Prozessverarbeitung in der One Identity Manager History Database (`DialogDatabase.ConnectionString`) erfolgt.
    - **Datenbankbenutzer**: Name des Datenbankbenutzers.
3. Wählen Sie den Tabreiter **Datenbank- oder Serverrolle** und weisen Sie die Rolle **Datenbank: Rolle für Datenarchivierung** zu.
4. Speichern Sie die Änderungen.

Der DBQueue Prozessor erzeugt in der One Identity Manager-Datenbank die Datenbankrolle **OneIMHistoryRoleDB** und den Datenbankbenutzer. Der Datenbankbenutzer wird mit der SQL Server Anmeldung verbunden und in die Datenbankrolle aufgenommen.

## Szenario 2

One Identity Manager History Database und One Identity Manager-Datenbank befinden sich auf verschiedenen Datenbankservern. Der Verbindungsserver wird durch den One Identity Manager Service der One Identity Manager History Database erzeugt.

HINWEIS: Wenn Sie mit dem **sa** arbeiten, sind keine weiteren Schritte erforderlich.

Wenn Sie mit abgestuften Berechtigungen auf Serverebene und Datenbankebene arbeiten, sind zusätzliche Berechtigungen zum Erstellen eines Verbindungsservers und für die Datenübernahme erforderlich.

- Um einen Verbindungsserver zu erstellen, benötigt der Benutzer, mit dem die Prozessverarbeitung in der One Identity Manager History Database (`DialogDatabase.ConnectionString`) erfolgt, die folgenden Berechtigungen auf Serverebene:
    - Berechtigung **alter any linked server**

      Die Berechtigung wird zum Erstellen und Löschen eines Verbindungsservers benötigt. Der Verbindungsserver ermöglicht die Ausführung verteilter Abfragen.

- Berechtigung **alter any login**

  Die Berechtigung wird zum Erstellen und Löschen einer Zuordnung von Anmeldenamen auf dem lokalen Server und einem Anmeldenamen auf dem Verbindungsserver benötigt.

- Erstellen Sie auf dem Datenbankserver, auf dem die One Identity Manager-Datenbank liegt, eine SQL Server Anmeldung für die Datenübernahme.
- Erstellen Sie im Designer in der One Identity Manager-Datenbank einen Datenbankbenutzer.

***Um den Datenbankbenutzer in der One Identity Manager-Datenbank einzurichten***

1. Wählen Sie im Designer die Kategorie **Basisdaten > Sicherheitseinstellungen > Datenbankserverberechtigungen > Datenbankserver-Anmeldungen**.
2. Klicken Sie und erfassen Sie folgende Informationen:
   - **Anmeldename**: SQL Server Anmeldung für die Datenübernahme.
   - **Datenbankbenutzer**: Datenbankbenutzer.
3. Wählen Sie den Tabreiter **Datenbank- oder Serverrolle** und weisen Sie die Rolle **Datenbank: Rolle für Datenarchivierung** zu.
4. Speichern Sie die Änderungen.

Der DBQueue Prozessor erzeugt in der One Identity Manager-Datenbank die Datenbankrolle **OneIMHistoryRoleDB** und den Datenbankbenutzer. Der Datenbankbenutzer wird mit der SQL Server Anmeldung verbunden und in die Datenbankrolle aufgenommen.

## Szenario 3

One Identity Manager History Database und One Identity Manager-Datenbank befinden sich auf verschiedenen Datenbankservern. Es wird ein Verbindungsserver bereitgestellt.

- Erstellen Sie auf dem Datenbankserver, auf dem die One Identity Manager-Datenbank liegt, eine SQL Server Anmeldung für die Datenübernahme.
- Erstellen Sie im Designer in der One Identity Manager-Datenbank einen Datenbankbenutzer.

***Um den Datenbankbenutzer in der One Identity Manager-Datenbank einzurichten***

1. Wählen Sie im Designer die Kategorie **Basisdaten > Sicherheitseinstellungen > Datenbankserverberechtigungen > Datenbankserver-Anmeldungen**.
2. Klicken Sie und erfassen Sie folgende Informationen:

   **Anmeldename**: SQL Server Anmeldung für die Datenübernahme.

   **Datenbankbenutzer**: Datenbankbenutzer.

3. Wählen Sie den Tabreiter **Datenbank- oder Serverrolle** und weisen Sie die Rolle **Datenbank: Rolle für Datenarchivierung** zu.
4. Speichern Sie die Änderungen.

Der DBQueue Prozessor erzeugt in der One Identity Manager-Datenbank die Datenbankrolle **OneIMHistoryRoleDB** und den Datenbankbenutzer. Der Datenbankbenutzer wird mit der SQL Server Anmeldung verbunden und in die Datenbankrolle aufgenommen.

- Richten Sie den Verbindungsserver ein und referenzieren Sie die SQL Server Anmeldung für die Datenübernahme.

  Um einen Verbindungsserver bereitzustellen, wird empfohlen, die SQL Prozeduren `sp_addlinkedserver`, `sp_setNetname` und `sp_addlinkedsrvlogin` zu nutzen.
- Halten Sie den Namen des Verbindungsserver bereit. Diesen benötigen Sie bei Bekanntgabe der Quelldatenbank in der One Identity Manager History Database.
- Aktivieren Sie in der One Identity Manager History Database den Konfigurationsparameter **HDB | UseNamedLinkedServer**.

# Hinweise zum Einsatz mehrerer SQL Server

WICHTIG: Befinden sich One Identity Manager History Database und One Identity Manager-Datenbank auf verschiedenen Servern werden nur gleiche Versions- und Patch-stände von Betriebssystem und Datenbanksystem unterstützt.

Befinden sich One Identity Manager History Database und One Identity Manager-Datenbank auf verschiedenen Datenbankservern sind auf beiden Servern folgende Voraussetzungen für die Datenübernahme zu gewährleisten:

- Start der Dienste **Microsoft Distributed Transaction Coordinator** (DTC), **RPC Client** und **Security Accounts Manager**
- Für die Netzwerkkommunikation zwischen den Servern prüfen Sie die Einstellungen der Firewall und passen Sie bei Bedarf die Einstellungen entsprechend der Empfehlungen des eingesetzten Betriebssystems an. Weitere Informationen finden Sie in der Dokumentation zum eingesetzten Betriebssystem.
- In den DTC-Sicherheitseinstellungen sollten folgenden Einstellungen aktiviert sein:
  - DTC-Netzwerkzugriff (Network DTC Access)
  - Remoteclients zulassen (Allow Remote Clients)
  - Eingehende zulassen (Allow Inbound)
  - Ausgehende zulassen (Allow Outbound)
  - Kein Authentifizierung erforderlich (No Authentication Required)

  Die Sicherheitseinstellungen konfigurieren Sie in der Microsoft Management Console im Snap-In Komponentendienste.

Werden große Datenmengen von der One Identity Manager-Datenbank in die One Identity Manager History Database übertragen, sollte auf dem Datenbankserver, der die One Identity Manager-Datenbank hält, das Timeout für Remoteabfragen erhöht werden. Die Standardeinstellung ist 600 Sekunden, was einer Wartezeit von zehn Minuten entspricht. Ist die Wartezeit abgelaufen, wird die Datenübertragung abgebrochen. Das Timeout für Remoteabfragen sollte sich am Ausführungsintervall das Zeitplans zur Datenübernahme orientieren.

Das Timeout für Remoteabfragen können Sie mit folgendem Statement abfragen:

```
select * from sys.configurations where name like '%remote query timeout%'
```

Um das Timeout für Remoteabfragen zu ändern, verwenden Sie folgendes Statement:

```
exec sp_configure 'remote query timeout (s)',<new value>
RECONFIGURE WITH OVERRIDE
```

Wobei:

```
<new value> = Neuer Timeout-Wert in Sekunden
```

# Hinweise zur Nutzung der integrierten Windows-Authentifizierung

Wird die integrierte Windows-Authentifizierung genutzt, erfolgt die Datenübernahme mit dem Benutzerkonto des One Identity Manager Service der One Identity Manager History Database.

- Für das Benutzerkonto richten Sie auf dem Datenbankserver eine SQL Server Anmeldung ein. Befinden sich One Identity Manager History Database und One Identity Manager-Datenbank auf verschiedenen Servern, richten Sie die SQL Server Anmeldung auf beiden Datenbankservern ein.
- Weisen Sie der SQL Server Anmeldung die benötigten Berechtigungen für die Datenübernahme zu. Weitere Informationen finden Sie unter Berechtigungen für die One Identity Manager History Database auf einem SQL Server auf Seite 6.

Befinden sich One Identity Manager History Database, One Identity Manager Service und One Identity Manager-Datenbank auf verschiedenen Servern sind weitere Voraussetzungen zu erfüllen:

- Das Benutzerkonto des One Identity Manager Service benötigt einen Service Principal Name (SPN) für die Authentifizierung. Dieser kann über folgenden Kommandozeilen erstellt werden:

  ```
  SetSPN -A HTTP/<Vollständiger Domänenname> <Domäne>\<Benutzerkonto>
  ```

- Das Benutzerkonto des One Identity Manager Service muss für Delegierungen freigeschaltet sein und Kerberos zur Authentifizierung verwenden.

  Setzen Sie dazu in der Microsoft Management Konsole für Active Directory Benutzer- und Computer auf dem Tabreiter **Delegierungen** die Option **Benutzer bei**

**Delegierungen aller Dienste vertrauen (nur Kerberos)** (Trust this user for delegation to any service (Kerberos only).

- Der SQL Server Dienst benötigt einen Service Principal Name zur Authentifizierung. Diesen können Sie über folgenden Kommandozeilenaufruf prüfen:

  ```
  SetSPN -L <Name des Datenbankservers>
  ```

# Einrichten eines One Identity Manager Service für die One Identity Manager History Database

Der Dienst One Identity Manager Service sorgt für die Datenübernahme aus der One Identity Manager-Datenbank in die One Identity Manager History Database.

Die Systemvoraussetzungen für die Installation der One Identity Manager Service auf einem Server und die erforderlichen Berechtigungen für das Dienstkonto sind im *One Identity Manager Installationshandbuch* beschrieben. Ausführliche Informationen zur Konfiguration des One Identity Manager Service finden Sie im *One Identity Manager Konfigurationshandbuch*.

Um den One Identity Manager Service auf einem Server zu installieren, haben Sie folgende Möglichkeiten:

- Richten Sie den Dienst bei der initialen Schemainstallation mit dem Configuration Wizard ein. Mit dem Configuration Wizard konfigurieren Sie den Dienst und installieren den Dienst remote auf einem Server. Ausführliche Informationen finden Sie *One Identity Manager Installationshandbuch*.
- Mit dem Server Installer können Sie einen Jobserver mit seinen Maschinenrollen und Serverfunktionen in der Datenbank erstellen. Mit dem Server Installer konfigurieren Sie den Dienst und installieren den Dienst remote auf einem Server. Ausführliche Informationen finden Sie *One Identity Manager Installationshandbuch*.
- Im Designer können Sie einen Jobserver mit die Maschinenrollen und Serverfunktionen erstellen, den Dienst auf dem Server konfigurieren und remote installieren. Ausführliche Informationen finden Sie *One Identity Manager Konfigurationshandbuch*.
- Falls eine Remote-Installation nicht möglich ist, können Sie die Dienstkomponenten mit dem Installationsassistenten lokal auf einem Server installieren. Weitere Informationen finden Sie unter Komponenten für die One Identity Manager History Database installieren auf Seite 22.

### Szenarien für die Verteilung des One Identity Manager Service auf Servern

- One Identity Manager Service für die One Identity Manager-Datenbank und One Identity Manager Service für die One Identity Manager History Database werden auf verschiedenen Servern installiert.
- One Identity Manager Service für die One Identity Manager-Datenbank und One Identity Manager Service für die One Identity Manager History Database werden auf einem Server installiert.

  Für dieses Szenario ändern Sie für den One Identity Manager Service für die One Identity Manager History Database das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung.

  - Wenn Sie die Dienstkomponenten mit dem Installationsassistenten lokal auf einem Server installieren, ändern Sie auf der Seite **Ändern der Service-Einstellungen** den Namen, den Anzeigenamen und die Beschreibung für den One Identity Manager Service für die One Identity Manager History Database. Weitere Informationen finden Sie unter Komponenten für die One Identity Manager History Database installieren auf Seite 22.
  - Wenn Sie den Dienst remote mit dem Configuration Wizard, mit dem Server Installer oder über den Designer installieren, können Sie während der Installation über erweiterte Optionen das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung für den One Identity Manager Service für die One Identity Manager History Database ändern.

### Verwandte Themen

- Installieren einer One Identity Manager History Database auf Seite 23

# Einrichten einer administrativen Arbeitsstation für den Zugriff auf die One Identity Manager History Database

Die Systemvoraussetzungen für die Installation einer administrativen Arbeitsstation und die erforderlichen Berechtigungen sind im *One Identity Manager Installationshandbuch* beschrieben.

Auf einer administrativen Arbeitsstation sollten Sie mindestens folgende Werkzeuge installieren:

- HistoryDB Manager
- Job Queue Info
- Designer

Auf der Arbeitsstation, auf der die Installation und Aktualisierung des One Identity Manager History Database Schemas gestartet wird, müssen zusätzlich die folgenden Voraussetzungen erfüllt sein:

- Installation des Configuration Wizard
- Zugriff auf die Installationsquellen

  HINWEIS: Wenn Sie die Installationsquellen auf ein Ablageverzeichnis kopieren, müssen Sie sicherstellen, dass die relative Verzeichnisstruktur erhalten bleibt.

Die Erstinstallation der One Identity Manager History Database-Werkzeuge auf den Arbeitsstationen nehmen Sie mit dem Installationsassistenten vor.

### Verwandte Themen

- Komponenten für die One Identity Manager History Database installieren auf Seite 22

# Komponenten für die One Identity Manager History Database installieren

***Um die Komponenten zu installieren***

1. Starten Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager Installationsmediums.
2. Wechseln Sie auf den Tabreiter **Andere Produkte,** wählen Sie den Eintrag **One Identity Manager History Database** und klicken Sie **Installieren**.
3. Der Installationsassistent wird gestartet. Auf der Startseite wählen Sie die Sprache für den Installationsassistenten aus und klicken Sie **Weiter**.
4. Bestätigen Sie die Lizenzbedingungen.
5. Auf der Seite **Einstellungen für die Installation** erfassen Sie folgenden Informationen.
   - **Installationsquelle**: Wählen Sie das Verzeichnis mit den Installationsdateien.
   - **Installationsverzeichnis**: Wählen Sie das Verzeichnis, in das die Dateien des One Identity Manager History Database installiert werden sollen.

     HINWEIS: Um weitere Konfigurationseinstellungen vorzunehmen, klicken Sie auf die Pfeil Schaltfläche neben dem Eingabefeld. Hier können Sie festlegen, ob die Installation auf einem 64 Bit- Betriebssystem oder auf einem 32 Bit-Betriebssystem erfolgt.

     Für eine Standardinstallation nehmen Sie keine weiteren Konfigurationseinstellungen vor.
6. Auf der Seite **Maschinenrolle zuordnen** legen Sie die Maschinenrollen fest.

HINWEIS: Bei Auswahl einer Maschinenrolle werden alle untergeordneten Installationspakete mit ausgewählt. Sie können einzelne Installationspakete abwählen.

7. Auf der Seite **Ändern der Service-Einstellungen** können Sie den Namen, den Anzeigenamen und die Beschreibung für die Installation des One Identity Manager Service ändern.

   HINWEIS: Diese Seite wird nur angezeigt, wenn Sie die Maschinenrolle **Server | Job Server** ausgewählt haben.

8. Auf der letzten Seite des Installationsassistenten können Sie verschiedene Programme für die weitere Installation starten.

   - Um die Installation des One Identity Manager History Database Schemas auszuführen, starten Sie den Configuration Wizard und folgen Sie den Anweisungen des Configuration Wizard.

     HINWEIS: Führen Sie diesen Schritt nur auf der Arbeitsstation aus, auf der Sie die Installation des One Identity Manager History Database Schemas starten.

9. Um den Installationsassistenten zu beenden, klicken Sie **Ende**.
10. Schließen Sie das Autorun Programm.

Der One Identity Manager wird für alle Benutzerkonten auf der Arbeitsstation oder dem Server installiert. In der Standardinstallation wird der One Identity Manager installiert unter:

- `%ProgramFiles(x86)%\One Identity` (auf 32-Bit Betriebssystemen)
- `%ProgramFiles%\One Identity` (auf 64-Bit Betriebssystemen)

# Installieren einer One Identity Manager History Database

WICHTIG: One Identity Manager-Datenbank und One Identity Manager History Database müssen den gleichen Versionsstand haben.

Die Installation einer One Identity Manager History Database ist ähnlich der Installation einer One Identity Manager-Datenbank. Ausführliche Informationen zu den Systemvoraussetzungen und zum Installieren einer Datenbank finden Sie *One Identity Manager Installationshandbuch*.

Die One Identity Manager History Database richten Sie mit dem Configuration Wizard ein.

HINWEIS: Beachten Sie folgende Besonderheiten:

- Im Configuration Wizard wählen Sie auf der Seite **Konfigurationsmodule auswählen** das Konfigurationsmodul.

    - Wenn Sie den Configuration Wizard über den Installationsassistenten gestartet haben, sind die Konfigurationsmodule für die gewählte Edition bereits aktiviert. Prüfen Sie in diesem Fall die Modulauswahl.
    - Wenn Sie den Configuration Wizard direkt gestartet haben, wählen Sie an dieser Stelle das **Modul Datenarchivierung**. Abhängige Konfigurationsmodule werden automatisch mit ausgewählt.
  - Wenn Sie den One Identity Manager Service für die One Identity Manager History Database mit dem Configuration Wizard installieren, können Sie auf der Seite **Dienstinstallation** über erweiterte Optionen das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung des Dienstes ändern.

Der Configuration Wizard führt die folgenden Schritte aus.

1. Installieren des One Identity Manager History Database Schemas in eine Datenbank.

   Der Configuration Wizard kann eine neue Datenbank erstellen und das Schema installieren. Alternativ kann das Schema in eine bereits bestehende Datenbank installiert werden.
2. Erstellen der erforderlichen SQL Server Anmeldungen und Datenbankbenutzer mit den Berechtigungen für den administrative Benutzer, Konfigurationsbenutzer und Endbenutzer.
3. Erstellen der administrativen Systembenutzer und Berechtigungsgruppen.
4. Verschlüsseln der Datenbank.
5. Installieren und Konfigurieren des One Identity Manager Service mit direktem Zugriff auf die One Identity Manager History Database für die Verarbeitung von SQL Prozessen.

Nach der Schemainstallation sind weitere Schritte zur Konfiguration der One Identity Manager History Database erforderlich.

- Konfigurieren Sie die Datenbank für eine Testumgebung, Entwicklungsumgebung oder den produktiven Einsatz. Ausführliche Informationen finden Sie *One Identity Manager Installationshandbuch*.
- Geben Sie die Quelldatenbank in der One Identity Manager History Database bekannt.
- Richten Sie das Archivierungsverfahren ein.

## Verwandte Themen

- Berechtigungen für die One Identity Manager History Database auf einem SQL Server auf Seite 6
- Berechtigungen für die One Identity Manager History Database in einer verwalteten Instanz in Azure SQL-Datenbank auf Seite 11
- Erweiterte Konfiguration für die Datenübernahme auf Seite 15
- Quelldatenbanken in der One Identity Manager History Database bekanntgeben auf Seite 28

- Einrichten eines One Identity Manager Service für die One Identity Manager History Database auf Seite 20
- Ablauf der Aktualisierung bei Freigabe einer neuen Version auf Seite 25

# Ablauf der Aktualisierung bei Freigabe einer neuen Version

WICHTIG: One Identity Manager-Datenbank und One Identity Manager History Database müssen den gleichen Versionsstand haben.

HINWEIS: Lesen Sie die Versionshinweise für eventuell abweichende oder zusätzliche Schritte zur Aktualisierung des One Identity Manager.

Ausführliche Informationen zum Aktualisieren einer Datenbank finden Sie *One Identity Manager Installationshandbuch*.

***Um die One Identity Manager History Database auf eine neue Version zu aktualisieren***

1. Führen Sie im Designer alle Konsistenzprüfungen im Bereich **Datenbank** aus.
    a. Starten Sie den Konsistenzeditor im Designer über den Menüeintrag **Datenbank > Datenkonsistenz überprüfen**.
    b. Klicken Sie im Dialog **Testeinstellungen** das Symbol .
    c. Aktivieren Sie alle Tests im Bereich **Datenbank** und klicken Sie **OK**.
    d. Starten Sie die Prüfung über das Menü **Konsistenztest > Starten**.

    Alle Datenbanktests müssen erfolgreich sein. Korrigieren Sie die Fehler. Einige Konsistenzprüfungen bieten Reparaturmethoden zur Fehlerkorrektur an.
2. Aktualisieren Sie die administrative Arbeitsstation, auf welcher die Schemaaktualisierung der One Identity Manager History Database gestartet wird.
    a. Führen Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager-Installationsmediums aus.
    b. Wechseln Sie auf den Tabreiter **Andere Produkte** und wählen Sie den Eintrag **One Identity Manager History Database**.
    c. Klicken Sie **Installieren**.

    Der Installationsassistent wird gestartet.
    d. Folgen Sie den Installationsanweisungen.

    WICHTIG: Wählen Sie auf der Seite **Einstellungen für die Installation** als Installationsverzeichnis, das Verzeichnis Ihrer bisherigen Installation. Anderenfalls erfolgt keine Aktualisierung der Komponenten, sondern eine Neuinstallation in einem zweiten Verzeichnis.
3. Beenden Sie den One Identity Manager Service auf dem Aktualisierungsserver.

4. Erstellen Sie eine Sicherung der One Identity Manager History Database.
5. Prüfen Sie, ob der Kompatibilitätsgrad der Datenbank auf den Wert **140** eingestellt ist und passen Sie die Wert bei Bedarf an.
6. Führen Sie die Schemaaktualisierung der One Identity Manager History Database aus.
    - Starten Sie den Configuration Wizard auf der administrativen Arbeitsstation.

      Verwenden Sie für die Aktualisierung des One Identity Manager Schemas mit dem Configuration Wizard einen Benutzer, der mindestens administrative Berechtigungen auf die One Identity Manager-Datenbank hat.

        - Verwenden Sie denselben Benutzer, den Sie auch für die initiale Schemainstallation verwendet haben.
        - Haben Sie bei der Schemainstallation einen administrativen Benutzer erstellt, dann verwenden Sie diesen Benutzer.
        - Haben Sie zur Schemainstallation einen Benutzer mit Windows-Authentifizierung gewählt, dann müssen Sie diesen Benutzer zur Aktualisierung verwenden.

      HINWEIS: Wenn Sie bei der Aktualisierung von Version 8.0.x auf die Version 8.2 auf das abgestufte Berechtigungskonzept wechseln möchten, verwenden Sie den Installationsbenutzer laut Berechtigungen für die One Identity Manager History Database auf einem SQL Server auf Seite 6.

      Passen Sie nach der Aktualisierung des One Identity Manager die Verbindungsparameter an. Die betrifft beispielsweise die Verbindungsinformationen für die Datenbank (`DialogDatabase`), den One Identity Manager Service, die Anwendungsserver, die Administrations- und Konfigurationswerkzeuge, die Webanwendungen und die Webservices sowie die Verbindungsinformationen in Synchronisationsprojekten.

      Wenn Sie bei der Aktualisierung von Version 8.1.x zu abgestuften Berechtigungen wechseln möchten, wenden Sie sich an den Support. Das Support Portal ist unter https://support.oneidentity.com/identity-manager/ erreichbar.
7. Aktualisieren Sie den One Identity Manager Service auf dem Aktualisierungsserver.
    a. Führen Sie die Datei `autorun.exe` aus dem Basisverzeichnis des One Identity Manager-Installationsmediums aus.
    b. Wechseln Sie auf den Tabreiter **Andere Produkte** und wählen Sie den Eintrag **One Identity Manager History Database**.
    c. Klicken Sie **Installieren**.

       Der Installationsassistent wird gestartet.
    d. Folgen Sie den Installationsanweisungen.

       WICHTIG: Wählen Sie auf der Seite **Einstellungen für die Installation** als Installationsverzeichnis, das Verzeichnis Ihrer bisherigen Installation.

Anderenfalls erfolgt keine Aktualisierung der Komponenten, sondern eine Neuinstallation in einem zweiten Verzeichnis.

8. Prüfen Sie die Anmeldeinformationen des One Identity Manager Service. Geben Sie das zu verwendende Dienstkonto an.
9. Starten Sie den One Identity Manager Service auf dem Aktualisierungsserver.

# 3

# Quelldatenbanken in der One Identity Manager History Database bekanntgeben

Für die Datenübernahme geben Sie in der One Identity Manager History Database die zu verwendende One Identity Manager-Datenbank bekannt. Nutzen Sie den HistoryDB Manager um den Zugriff auf die Quelldatenbanken einzurichten.

***Um eine Quelldatenbank bekanntzugeben***

1. Starten Sie den HistoryDB Manager und geben Sie die Verbindungsdaten an.
2. Wählen Sie die Kategorie **Historie > Basisdaten > Quelldatenbanken**.
3. Wählen Sie in der Ergebnisliste die Quelldatenbank aus und bearbeiten Sie die Stammdaten.
   - **Server**: Name des Datenbankservers, auf dem sich die One Identity Manager-Datenbank befindet.

     Den Servernamen können Sie in der One Identity Manager-Datenbank über folgende Abfrage ermitteln:

     ```
     select @@SERVERNAME
     ```

     HINWEIS:
     - Wenn der Server über einen bestimmten Port erreichbar ist, können Sie den Port folgendermaßen übergeben.

       ```
       Servername, Port
       ```

     - Wenn Sie einen Verbindungsserver bereitstellen, tragen Sie den Namen des Verbindungsservers ein.
   - **Datenbank**: Name der One Identity Manager-Datenbank.
   - **Datenbank-ID**: Datenbank-ID der One Identity Manager-Datenbank. Diese Kennung entspricht der UID des Datenbankeintrages in der One Identity Manager-Datenbank.

     HINWEIS: Verbinden Sie sich mit dem Object Browser auf die One Identity Manager-Datenbank und kopieren Sie aus der Tabelle `DialogDatabase` und den

Wert der Spalte `UID_Database`. Diesen Wert fügen Sie im Eingabefeld **Datenbank-ID** ein.

- (Optional) **Integrierte Windows Authentifizierung verwenden**: Wird die integrierte Windows-Authentifizierung genutzt, erfolgt die Datenübernahme mit dem Benutzerkonto des One Identity Manager Service. Für den Einsatz dieses Authentifizierungsverfahrens sind bestimmte Installationsvoraussetzungen zu beachten.
- **Datenbankbenutzer** und **Kennwort**: SQL Server Anmeldung und Kennwort für die Datenübernahme.

  Diese Angabe ist nur erforderlich, wenn sich One Identity Manager History Database und One Identity Manager-Datenbank auf unterschiedlichen Servern befinden und kein Verbindungsserver bereitgestellt wird.

4. Speichern Sie die Änderungen.

## Verwandte Themen

- Hinweise zur Nutzung der integrierten Windows-Authentifizierung auf Seite 19
- Erweiterte Konfiguration für die Datenübernahme auf Seite 15

# 4

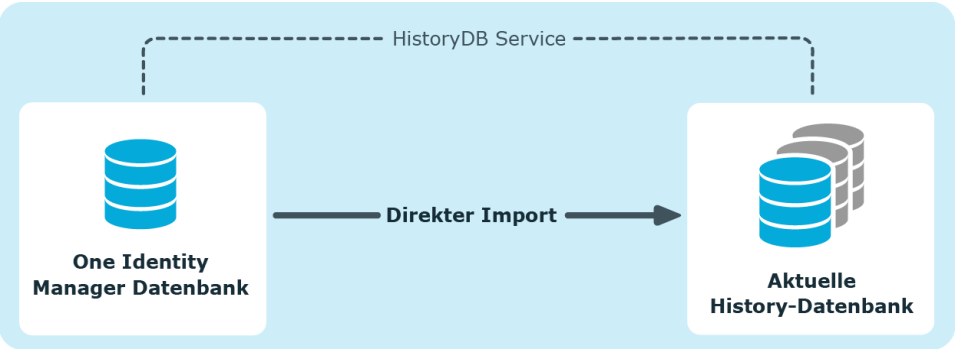
# Einrichten des Archivierungsverfahrens

Alle im One Identity Manager protokollierten Aufzeichnungen werden zunächst in der One Identity Manager-Datenbank gespeichert. Der Anteil der historisierten Daten am Gesamtvolumen einer One Identity Manager-Datenbank sollte maximal 25 % betragen. Anderenfalls kann es zu Performance-Problemen kommen. Die Aufzeichnungen sollten in regelmäßigen Abständen aus der One Identity Manager-Datenbank entfernt und archiviert werden.

Um die aufgezeichneten Daten in regelmäßigen Abständen aus der One Identity Manager-Datenbank zu entfernen, werden folgende Verfahren angeboten:

- Die Daten können direkt aus der One Identity Manager-Datenbank in eine One Identity Manager History Database übernommen werden. Dieses ist das Standardverfahren für die Datenarchivierung. Wählen Sie dieses Verfahren, wenn die Server auf denen die One Identity Manager-Datenbank und die One Identity Manager History Database liegen, einander sehen.
- Die Daten werden ohne Archivierung nach einer festgelegten Zeitspanne aus der One Identity Manager-Datenbank gelöscht.

**Abbildung 1: Übernahme der Aufzeichnungen in eine One Identity Manager History Database**




Für die direkte Übernahme in eine History Database werden in der One Identity Manager-Datenbank alle Aufzeichnungen, die von einer Aktion ausgelöst wurden, anhand einer ID-Nummer, der GenProcID, zu einer Prozessgruppe zusammengefasst. Nach erfolgreichem

Export werden die exportierten Prozessgruppen mit den zugehörigen Aufzeichnungen aus der One Identity Manager-Datenbank gelöscht.

Für die direkte Übernahme in eine One Identity Manager History Database müssen folgende Bedingungen erfüllt sein:

- Der Teilbereich der Aufzeichnungen ist für den Export konfiguriert.
- Die Aufbewahrungszeit aller Aufzeichnungen, die zu einer Prozessgruppe gehören, ist abgelaufen, unabhängig davon ob der Teilbereich zum Export gekennzeichnet ist.
- Es gibt keine aktiven Prozesse mit der GenProcID der Prozessgruppe in der DBQueue, in der Jobqueue oder als geplante Operationen.
- Es gibt für die auslösende Aktion mindestens eine Aufzeichnung in dem Teilbereich, der exportiert werden soll.

Für die Archivierung der Aufzeichnungen in eine One Identity Manager History Database sind in beiden Datenbanken - der One Identity Manager-Datenbank und der One Identity Manager History Database - Konfigurationen vorzunehmen.

# Auswahl des Archivierungsverfahrens in der One Identity Manager-Datenbank

Die Auswahl des grundlegenden Verfahrens treffen Sie über die Einstellung des Konfigurationsparameters **Common | ProcessState | ExportPolicy**. Passen Sie den Konfigurationsparameter im Designer an.

- Ist der Konfigurationsparameter deaktiviert, verbleiben die Daten in der One Identity Manager-Datenbank.
- Ist der Konfigurationsparameter aktiviert, dann wird das gewählte Verfahren angewendet.
    - **HDB**: Die Daten werden nach Ablauf einer festgelegten Zeitspanne direkt in eine One Identity Manager History Database übernommen.
    - **NONE**: Die Daten werden nach Ablauf einer festgelegten Zeitspanne aus der One Identity Manager-Datenbank gelöscht.

Für jeden Teilbereich der Aufzeichnungen können Sie nach der Auswahl des grundlegenden Verfahrens separat festlegen, ob die Daten exportiert oder gelöscht werden. Die Festlegung für die einzelnen Bereiche treffen Sie über Konfigurationsparameter. Passen Sie die Konfigurationsparameter im Designer an.

**Tabelle 1: Konfigurationsparameter für die Behandlung der aufgezeichneten Informationen**

| Konfigurationsparameter | Bedeutung |
|---|---|
| Common \| ProcessState \| | Die aufgezeichneten Datenänderungen sollen exportiert |

| Konfigurationsparameter | Bedeutung |
|---|---|
| PropertyLog \| IsToExport | werden. Ist der Konfigurationsparameter nicht aktiv, werden die Informationen nach Ablauf der Aufbewahrungszeit gelöscht. |
| Common \| ProcessState \| ProgressView \| IsToExport | Die Prozessinformationen sollen exportiert werden. Ist der Konfigurationsparameter nicht aktiv, werden die Informationen nach Ablauf der Aufbewahrungszeit gelöscht. |
| Common \| ProcessState \| JobHistory \| IsToExport | Die Informationen in der Prozesshistorie sollen exportiert werden. Ist der Konfigurationsparameter nicht aktiv, werden die Informationen nach Ablauf der Aufbewahrungszeit gelöscht. |

# Festlegen der Aufbewahrungszeiten

Die Aufzeichnungen werden, abhängig vom gewählten Archivierungsverfahren, nach Ablauf der Aufbewahrungszeiten aus der One Identity Manager-Datenbank exportiert oder gelöscht. Für die Teilbereiche, deren Aufzeichnungen exportiert werden, sollte eine längere Aufbewahrungszeit gewählt werden, als für die Teilbereiche, deren Aufzeichnungen gelöscht werden.

HINWEIS: Wenn Sie keine Aufbewahrungszeiten festlegen, werden die Aufzeichnungen dieser Teilbereiche täglich innerhalb der tägliche Wartungsaufträge des DBQueue Prozessors aus der One Identity Manager-Datenbank gelöscht.

Die Aufzeichnungen werden erst exportiert, wenn die Aufbewahrungszeiten aller Teilbereiche abgelaufen ist und keine weiteren aktiven Prozesse für die Prozessgruppe (GenProcID) in der DBQueue, der Prozesshistorie oder als geplante Operation existieren.

Die Aufbewahrungszeiten für die einzelnen Bereiche legen Sie über Konfigurationsparameter fest. Passen Sie den Konfigurationsparameter im Designer an.

**Tabelle 2: Konfigurationsparameter für die Aufbewahrungszeiten**

| Konfigurationsparameter | Bedeutung |
|---|---|
| Common \| ProcessState \| PropertyLog \| LifeTime | Mit diesem Konfigurationsparameter wird die maximale Aufbewahrungszeit für aufgezeichnete Datenänderungen in der Datenbank festgelegt. |
| Common \| ProcessState \| ProgressView \| LifeTime | Mit diesem Konfigurationsparameter wird die maximale Aufbewahrungszeit für Prozessinformationen in der Datenbank festgelegt. |
| Common \| ProcessState \| JobHistory \| LifeTime | Mit diesem Konfigurationsparameter wird die maximale Aufbewahrungszeit für Aufzeichnungen aus der Prozesshistorie in der Datenbank festgelegt. |

### Beispiel 1

Die Aufzeichnungen werden direkt in eine One Identity Manager History Database übernommen. Für die einzelnen Teilbereiche wurden folgende Konfigurationen gewählt:

| Konfiguration | Prozess-informationen | Prozess-historie | Daten-änderungen |
|---|---|---|---|
| Daten exportieren | Nein | Nein | Ja |
| Aufbe-wahrungszeit | 3 Tage | 4 Tage | 5 Tage |

Daraus ergibt sich folgender Ablauf:

| Zeitpunkt | Prozessinformationen | Prozesshistorie | Datenänderungen |
|---|---|---|---|
| Tag 3 | Daten werden in der One Identity Manager-Datenbank gelöscht. | Keine Aktion. | Keine Aktion. |
| Tag 4 | - | Daten werden in der One Identity Manager-Datenbank gelöscht. | Keine Aktion. |
| Tag 5 | - | - | Daten werden in die One Identity Manager History Database übernommen und anschließend in der One Identity Manager-Datenbank gelöscht. |

### Beispiel 2

Die Aufzeichnungen werden direkt in eine One Identity Manager History Database übernommen. Für die einzelnen Teilbereiche wurden folgende Konfigurationen gewählt:

| Konfiguration | Prozess-informationen | Prozess-historie | Daten-änderungen |
|---|---|---|---|
| Daten exportieren | Ja | Nein | Ja |
| Aufbe-wahrungszeit | 3 Tage | 4 Tage | 5 Tage |

Daraus ergibt sich folgender Ablauf:

| Zeitpunkt | Prozessinformationen | Prozesshistorie | Datenänderungen |
|---|---|---|---|
| Tag 3 | Keine Aktion, da die Aufbewahrungszeit noch nicht in allen Teilbe-reichen abgelaufen ist. | Keine Aktion. | Keine Aktion. |
| Tag 4 | Keine Aktion, da die Aufbewahrungszeit noch nicht in allen Teilbe-reichen abgelaufen ist. | Daten werden in der One Identity Manager-Datenbank gelöscht. | Keine Aktion. |
| Tag 5 | Daten werden exportiert und anschließend gelöscht. | - | Daten werden in die One Identity Manager History Database übernommen und anschließend in der One Identity Manager-Datenbank gelöscht. |

# Konfigurieren der Datenbanken für die Archivierung

### Konfigurieren der One Identity Manager-Datenbank

- Aktivieren Sie im Designer den Konfigurationsparameter **Common | ProcessState | ExportPolicy** und tragen Sie den Wert **HDB** ein.
- Konfigurieren Sie die Teilbereiche für den Export und legen Sie die Aufbewahrungszeiten fest.
- Prüfen Sie im Designer den Wert der Konfigurationsparameters **Common | ProcessState | PackageSizeHDB**. Dieser Parameter legt die maximale Anzahl der

Prozessgruppen fest, die in die One Identity Manager History Database übertragen werden. Der Standardwert ist **10000**.

### Konfigurieren der One Identity Manager History Database

- Geben Sie in der One Identity Manager History Databasedie One Identity Manager-Datenbank als Quelldatenbank bekannt.
- Der Import wird in regelmäßigen Abständen durch den One Identity Manager Service der One Identity Manager History Database ausgeführt. Konfigurieren und aktivieren Sie im Designer den Zeitplan **Prozessinformationen direkt importieren**.

### Verwandte Themen

- Auswahl des Archivierungsverfahrens in der One Identity Manager-Datenbank auf Seite 31
- Festlegen der Aufbewahrungszeiten auf Seite 32
- Quelldatenbanken in der One Identity Manager History Database bekanntgeben auf Seite 28

# Löschen der Aufzeichnungen in der One Identity Manager-Datenbank ohne Archivierung

Sollen die Aufzeichnungen einzelner Teilbereiche für einen gewissen Zeitraum in der One Identity Manager-Datenbank gehalten werden, jedoch keine spätere Archivierung erfolgen, dann haben Sie folgende Möglichkeiten:

- Um einen einzelnen Teilbereich von der Archivierung auszuschließen, konfigurieren Sie diesen Teilbereich nicht für den Export, sondern legen nur den Aufbewahrungszeitraum fest.
- Um alle Teilbereiche ohne Archivierung direkt zu löschen, legen Sie die Aufbewahrungszeiten fest. Aktivieren Sie im Designer den Konfigurationsparameter **Common | ProcessState | ExportPolicy** und tragen Sie den Wert **NONE** ein.

Die Aufzeichnungen werden nach Ablauf der Aufbewahrungszeit durch den DBQueue Prozessor aus der One Identity Manager-Datenbank gelöscht. Zusätzlich werden alle Einträge für ausgelöste Aktionen gelöscht, zu denen es keine Aufzeichnungen in den Teilbereichen gibt.

HINWEIS: Wenn Sie keine Aufbewahrungszeiten festlegen, werden die Aufzeichnungen dieser Teilbereiche innerhalb der täglichen Wartungsaufträge des DBQueue Prozessor aus der One Identity Manager-Datenbank gelöscht.

### Verwandte Themen

- Auswahl des Archivierungsverfahrens in der One Identity Manager-Datenbank auf Seite 31
- Festlegen der Aufbewahrungszeiten auf Seite 32
- Performance-Optimierung zum Löschen von Aufzeichnungen auf Seite 36

# Performance-Optimierung zum Löschen von Aufzeichnungen

Bei großen Datenmengen können Sie zur Performance-Optimierung die Menge der zu löschenden Objekte pro Operation und Verarbeitungslauf des DBQueue Prozessor festlegen. Die Festlegung für die einzelnen Bereiche treffen Sie über Konfigurationsparameter.

**Tabelle 3: Konfigurationsparameter für das Löschen der aufgezeichneten Datenänderungen**

| Konfigurationsparameter | Bedeutung |
|---|---|
| Common \| ProcessState \| PropertyLog \| Delete | Erlaubt die Konfiguration des Löschverhaltens für aufgezeichnete Datenänderungen. |
| Common \| ProcessState \| PropertyLog \| Delete \| BulkCount | Anzahl der Einträge, die in einer Operation gelöscht werden sollen. Standardwert ist **200**. |
| Common \| ProcessState \| PropertyLog \| Delete \| TotalCount | Gesamtmenge der Einträge, die in einem Verarbeitungslauf gelöscht werden sollen. Standardwert ist **10000**. |

**Tabelle 4: Konfigurationsparameter für das Löschen der Prozessinformationen**

| Konfigurationsparameter | Bedeutung |
|---|---|
| Common \| ProcessState \| ProgressView \| Delete | Erlaubt die Konfiguration des Löschverhaltens für Prozessinformationen. |
| Common \| ProcessState \| ProgressView \| Delete \| BulkCount | Anzahl der Einträge, die in einer Operation gelöscht werden sollen. Standardwert ist **200**. |
| Common \| ProcessState \| ProgressView \| Delete \| TotalCount | Gesamtmenge der Einträge, die in einem Verarbeitungslauf gelöscht werden sollen. Standardwert ist **10000**. |

**Tabelle 5: Konfigurationsparameter für das Löschen der Prozesshistorie**

| Konfigurationsparameter | Bedeutung |
|---|---|
| Common \| ProcessState \| JobHistory \| Delete | Erlaubt die Konfiguration des Löschverhaltens für die Prozesshistorie. |
| Common \| ProcessState \| JobHistory \| Delete \| BulkCount | Anzahl der Einträge, die in einer Operation gelöscht werden sollen. Standardwert ist **200**. |
| Common \| ProcessState \| JobHistory \| Delete \| TotalCount | Gesamtmenge der Einträge, die in einem Verarbeitungslauf gelöscht werden sollen. Standardwert ist **10000**. |

**Tabelle 6: Konfigurationsparameter für das Löschen von Prozessstatus-Einträge**

| Konfigurationsparameter | Bedeutung |
|---|---|
| Common \| ProcessState \| Delete | Erlaubt die Konfiguration des Löschverhaltens für die Einträge zum Prozessstatus. |
| Common \| ProcessState \| Delete \| BulkCount | Anzahl der Einträge, die in einer Operation gelöscht werden sollen. Standardwert ist **500**. |
| Common \| ProcessState \| Delete \| TotalCount | Gesamtmenge der Einträge, die in einem Verarbeitungslauf gelöscht werden sollen. Standardwert ist **10000**. |

# Über uns

One Identity Lösungen eliminieren die Komplexität und die zeitaufwendigen Prozesse, die häufig bei der Identity Governance, der Verwaltung privilegierter Konten und dem Zugriffsmanagement aufkommen. Unsere Lösungen fördern die Geschäftsagilität und bieten durch lokale, hybride und Cloud-Umgebungen eine Möglichkeit zur Bewältigung Ihrer Herausforderungen beim Identitäts- und Zugriffsmanagement.

## Kontaktieren Sie uns

Bei Fragen zum Kauf oder anderen Anfragen, wie Lizenzierungen, Support oder Support-Erneuerungen, besuchen Sie https://www.oneidentity.com/company/contact-us.aspx.

## Technische Supportressourcen

Technische Unterstützung steht für One Identity Kunden mit einem gültigen Wartungsvertrag und Kunden mit Testversionen zur Verfügung. Sie können auf das Support Portal unter https://support.oneidentity.com/ zugreifen.

Das Support Portal bietet Selbsthilfe-Tools, die Sie verwenden können, um Probleme schnell und unabhängig zu lösen, 24 Stunden am Tag, 365 Tage im Jahr. Das Support Portal ermöglicht Ihnen:

- Senden und Verwalten von Serviceanfragen
- Anzeigen von Knowledge Base Artikeln
- Anmeldung für Produktbenachrichtigungen
- Herunterladen von Software und technischer Dokumentation
- Anzeigen von Videos unter www.YouTube.com/OneIdentity
- Engagement in der One Identity Community
- Chat mit Support-Ingenieuren
- Anzeigen von Diensten, die Sie bei Ihrem Produkt unterstützen

# Index

## D



## O



## P